Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03100721.4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr: / Application no.: 03100721.4 / Demande no:

Anmeldetag: / Date of filing: 20.03.03 / Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Corporate Intellectual Property GmbH
Habsburgerallee 11
52064 Aachen
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Elektronisches Speicherbauteil oder Speichermodul und Verfahren zum Betreiben desselben

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

DE/21.11.02/DE 10254324

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G11C/

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT SE SI SK TR LI

BESCHREIBUNG

Elektronisches Speicherbauteil oder Speichermodul und Verfahren zum Betreiben desselben

Die vorliegende Erfindung betrifft allgemein das technische Gebiet der elektronischen Bauteile, insbesondere der mikroelektronischen Bauteile.

Im speziellen betrifft die vorliegende Erfindung ein elektronisches Speicherbauteil oder Speichermodul, aufweisend mindestens einen Speicherzellenbereich, in dem reguläre Daten repräsentierende physikalische Zustände mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming-Code, beschreibenden Abbildungsfunktion abgebildet sind.

Im speziellen betrifft die vorliegende Erfindung des weiteren ein Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils oder Speichermoduls der vorgenannten Art.

Elektronische Speicherbauelemente, wie zum Beispiel

- E[rasable]P[rogrammable]R[ead]O[nly]M[emories],
- E[lectrically]E[rasable]P[rogrammable]R[ead]O[nly]M[emories],
- Flash-Speicher,
- R[ead]O[nly]M[emories] oder
- R[andom]A[ccess]M[emories],

erlauben das Programmieren bzw. Schreiben und/oder das Lesen von digitalen Daten der Form "1" und "0", die häufig als geschriebener bzw. gelöschter Zustand (Bit) bezeichnet werden. Durch Abnutzung, durch äußere Einflüsse oder durch andere Ursachen kann es gelegentlich zu einem fehlerhaften Lesen dieser Daten kommen.

Diesem fehlerhaften Lesen der Daten kann zum Beispiel durch den Einsatz eines Fehlerkorrekturcodes entgegengewirkt werden, bei dem die Information redundant auf dem physikalischen Medium abgespeichert wird und ein Algorithmus beim Einlesen der Daten eben diese Daten auf Fehler hin untersucht.

Typischerweise werden Algorithmen verwendet, die in einem Speicherblock von zum Beispiel acht logischen Bits (, denen dann mehr als acht physikalische Bits entsprechen,) ein oder mehrere fehlerhafte Bits erkennen und/oder korrigieren können. Die Zuordnung der physikalisch gespeicherten Bits P (= physikalische Repräsentation) eines Speicherblocks zu den logisch ausgelesenen Bits K (= Benutzerrepräsentation) des Speicherblocks wird als Abbildungsfunktion A des Fehlerkorrekturcodes bezeichnet.

In Figur 1 ist in schematischer Blockdarstellung der von der Abbildungsfunktion A des Fehlerkorrekturcodes vermittelte konventionelle Zusammenhang gemäß dem Stand der Technik zwischen den physikalisch implementierten Bits P und den für den Benutzer verfügbaren, gegebenenfalls fehlerkorrigierten Bits K dargestellt. Bekannte Beispiele für derartige Fehlerkorrekturcodes sind Hamming-Codes.

Bei einem Hamming-Code handelt es sich grundsätzlich um einen Fehlerkorrekturcode, bei dem der Unterschied im Bitaufbau von Zeichen zu Zeichen besonders groß ist, um bei fehlerhafter Datenübertragung die Wahrscheinlichkeit einer vollständigen Korrektur des Zeichens zu maximieren. Mit dem Hamming-Code, bei dem Prüfstellen aus unterschiedlichen Paritätsprüfungen gewonnen werden können, ist es grundsätzlich möglich, Codes zur Korrektur von mehr als einem Fehler zu konstruieren. Beim Hamming-Code wird nur ein Teil der Informationsstellen im Codewort oder Datenwort auf gerade Parität ergänzt.

Allerdings kann der zur Fehlererkennung verwendete Algorithmus in der Praxis aus Effizienz- und Kostengründen niemals alle prinzipiell möglichen Fehler erkennen, sondern ist immer auf die Erkennung und eventuelle Korrektur von relativ wenigen Bits pro Speicherblock beschränkt. Diese konventionelle fehlertolerante Kodierung der Daten reicht in sicherheitskritischen Anwendungen nicht immer aus, insbesondere dann nicht, wenn einige charakteristische Fehlermuster in den Bits sehr viel häufiger als andere Fehlermuster auftreten oder auch sich durch externe Manipulation gezielt herstellen lassen.

So muss zum Beispiel bei der Kodierung des Zählers für das auf einer Geldkarte eingetragene Geld immer darauf geachtet werden, dass der physikalisch stabile Zustand, das heißt der Zustand, in den der Datenspeicher durch physikalische Prozesse nach einer Vielzahl von Jahren kippen könnte, einem leeren Kontostand entspricht, damit die Geldkarte nicht unbefugterweise mit mehr Geld nachgeladen werden kann.

Auch ist es mit dem Stand der Technik nicht einfach realisierbar, unbeschriebene Speicherblöcke von schon einmal beschriebenen Speicherblöcken zu unterscheiden. Dies ist beispielsweise im Bereich der SmartCards ein potentielles Sicherheitsrisiko.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein elektronisches Speicherbauteil oder Speichermodul der eingangs genannten Art sowie ein diesem elektronischen Speicherbauteil oder Speichermodul zugeordnetes Verfahren der eingangs genannten Art so weiterzubilden, dass zum einen die Wahrscheinlichkeit einer Fehlererkennung deutlich erhöht ist und zum anderen unbeschriebene Speicherblöcke in zuverlässiger Weise von schon einmal beschriebenen Speicherblöcken unterschieden werden können.

Diese Aufgabe wird durch ein elektronisches Speicherbauteil oder Speichermodul mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein Verfahren mit den im Anspruch 11 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung wird mithin ein völlig neuartiger Ansatz für einen mikroelektronischen Speicherbaustein (mikroelektronisches Speicherbauteil, mikroelektronisches Speichermodul) mit redundanter Datenkodierung zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen Zuständen offenbart.

Hierfür weist die den Fehlerkorrekturcode, zum Beispiel einen Hamming-Code (= Fehlerkorrekturcode, mit dem ein fehlerhaftes Bit innerhalb eines Datenblocks korrigiert werden kann --> sogenannte Ein-Fehler-Korrektur), beschreibende Abbildungsfunktion zumindest die spezielle Eigenschaft auf, dass es zusätzlich zum Abbilden sämtlicher "normalen", die regulären Daten repräsentierenden physikalischen Zustände im Speicher mindestens einen weiteren physikalischen Zustand gibt, der einen Ausnahme- oder Sonderzustand darstellt und der anhand seines Bitmusters auf jeden Fall erkannt werden kann, unabhängig davon, ob für die "normalen" Zustände, das heißt für die regulären Daten nur eine eingeschränkte Fehlererkennung bzw. Fehlerkorrektur möglich sein sollte oder ob die Fehlererkennung bzw. Fehlerkorrektur für die "normalen" Zustände nicht eingeschränkt wird.

Zweckmäßigerweise wird dieser weitere physikalische Zustand (oder werden diese weiteren physikalischen Zustände) so gewählt, dass unvermeidlichen physikalischen Einschränkungen des Speichermediums Rechnung getragen wird; so kann zum Beispiel in einem EEPROM der Zustand, in dem die Speicherzellentransistoren eines jeden Bits ausgeschaltet sind und nur Leckströme fließen, als ein spezieller Ausnahme- oder Sonderzustand festgelegt werden. Die Implementierung des Fehlerkorrekturcodes und die möglichen Reaktionen auf die verschiedenen Zustände kann in Hardware oder in Software erfolgen.

Mit den vorbeschriebenen Maßnahmen ist es zum Beispiel möglich, einen Speicherblock als noch nicht beschrieben zu markieren, indem dieser Zustand als spezieller Ausnahme- oder Sonderzustand im Fehlerkorrekturcode festgelegt wird. Im Beispiel der Geldkarte bietet es sich an, den physikalisch stabilen Zustand (, der sich nach vielen Jahren einstellen könnte, wenn keine Gegenmaßnahmen getroffen werden,) als "nicht beschrieben" zu definieren.

Gemäß einer bevorzugten Ausgestaltung der vorliegenden Erfindung können zudem alle weiteren physikalischen Zustände, die sich durch Manipulation des Speichers, wie zum Beispiel durch Bestrahlen mit elektromagnetischen Teilchen oder Wellen, auf relativ

einfache Weise herstellen lassen, als Ausnahme- oder Sonderzustände im Fehlerkorrekturcode gekennzeichnet werden. Diese Zustände können dann von der Software und/oder von der Hardware der Geldkarte eindeutig erkannt werden, so dass Manipulationen des Speichers entgegengewirkt werden kann.

Mit im wesentlichen der gleichen Methode lassen sich auch sicherheitsrelevante Daten oder Merkmale eines Chips schützen, zum Beispiel indem dieser Bereich so ausgelegt wird, dass im Normalbetrieb keine Ausnahme- oder Sonderzustände auftreten können, dass aber andererseits zum Beispiel das Löschen eines Speicherblocks in diesem Bereich einen Ausnahme- oder Sonderzustand generiert.

Dieser Ausnahme- oder Sonderzustand in einem sicherheitsrelevanten, in bevorzugter Weise in mindestens ein dotiertes Aufnahmesubstrat eingebetteten und/oder eingelassenen Speicherbereich kann dann erkannt werden, woraufhin entsprechende Maßnahmen, wie etwa eine "hardware exception" oder Modus-Änderungen, durch die kontrollierende C[entral]P[rocessing]U[nit] ausgeführt werden, um die Sicherheit des gesamten Speicherinhalts und Chips zu gewährleisten. In besonders vorteilhafter Weise lassen sich durch diese Technik EEPROM-Fuses schützen (zum Beispiel Konfiguration- und Trimwerte), die unter anderem den Grad der Verriegelung eines SmartCard-Chips festlegen.

Im Rahmen der vorliegenden Erfindung ist es durchaus möglich, die Speicherblocks bewusst mit einem Ausnahme- oder Sonderzustand zu beschreiben, zum Beispiel um sie als unbeschrieben zu markieren oder, wie im Falle des EEPROMs, um viele Blocks erst einmal schnell mit "Null" zu initialisieren. Dies hat den Vorteil, dass beim nachfolgenden Schreiben nur noch die Hälfte der Zeit benötigt wird, weil keine Vorinitialisierung mehr erforderlich ist. In einem solchen Fall existieren dann zum Beispiel zwei verschiedene, der Null entsprechende Zustände, nämlich der Ausnahme- oder Sonderzustand "gelöscht" und das eigentliche Datum "Null"; beim Lesen verhalten sich diese beiden "Nullen" unterschiedlich.

Eine erfindungsgemäß erhöhte Wahrscheinlichkeit der Fehlererkennung ist auch im Hinblick auf das Detektieren und Verfolgen potentieller Angriffe auf das Speicherbauteil oder Speichermodul von großer Bedeutung, denn nicht zuletzt sind Speicherbauteile oder Speichermodule in sicherheitssensitiven Anwendungen, wie etwa Chipkarten, SmartCard-Controllern oder dergleichen, häufig das Ziel verschiedener möglicher Attacken.

Während in diesem Zusammenhang "reine" sicherheitsrelevante Daten in einfacher Weise (software-)algorithmisch geschützt und überprüft werden können, ist ein (software-)algorithmisches Schützen und Überprüfen für ausführbaren Programmcode nicht praktikabel, nicht zuletzt angesichts der Sensitivität von ausführbarem Programmcode in bezug auf Modifikationen; auch für im Speicherzellenbereich gegebenenfalls abgelegte Betriebsparameter oder dergleichen ist eine Lösung auf Softwarebasis nicht sinnvoll.

Grundsätzlich sind verschiedene Angriffe denkbar, die den Inhalt des Speicher(zellenbereich)s verändern oder die den Lesevorgang derart manipulieren, dass veränderte Daten bzw. falsche Programmbefehle ausgelesen werden. Zum Erhöhen der Lebensdauer von Speicherbauteilen oder von Speichermodulen wird häufig eine Fehlerkorrekturschaltung eingesetzt, die es beispielsweise ermöglicht, Ein-Bit-Fehler zu erkennen und zu korrigieren. Eine solche Fehlerkorrekturschaltung wird in modifizierter Form zusätzlich zum Erkennen einer Reihe von möglichen Angriffen verwendet, was eine Reaktion, etwa ein Deaktivieren des Chips, ermöglicht.

Eine mögliche Attacke ist das Beleuchten des Speicherbauteils oder Speichermoduls mit elektromagnetischen Wellen, insbesondere mit Licht. Als Gegenmaßnahme werden zum Beispiel Lichtsensoren auf dem Chip integriert und die sensitiven Schaltungsteile sowie der Speicherzellenbereich mit Metall weitestgehend abgedeckt, um Auswirkungen durch Beleuchten zu verhindern. Denkbar sind auch zusätzliche Bits, die explizit als Sensor verwendet werden können, oder zwischenzeitlich vorgenommene Lesezugriffe ohne Selektion eines Bytes.

Das Abdeckeln mit Metall verhindert nicht, dass das Speicherbauteil oder Speichermodul mit Licht geeigneter Wellenlänge durch das Substrat hindurch, also "von hinten" beleuchtet werden kann. Denkbar ist auch, dass bei hoher Intensität die Metallabdeckung nicht mehr ausreicht. Lichtsensoren decken nur Teile der Chipfläche ab; eine lokale Beleuchtung kann somit gegebenenfalls gar nicht festgestellt werden.

Zusätzliche Bits erhöhen die Fläche der Speichermatrix oder des Speicherzellenbereichs erheblich, ohne die lokale Sensitivität im Vergleich zur nachstehend vorgestellten, besonders erfinderischen Weiterbildung zu erhöhen. Zusätzliche Lesezugriffe können auch Angriffe auf einzelne Bits erkennen, sind jedoch durch die sequentielle Ausführung der zwei Lesezugriffe bei zeitlich variierenden Störungen unzuverlässiger und verdoppeln die Zugriffszeit auf den Speicher.

Demzufolge betrifft die vorliegende Erfindung des weiteren eine zum zusätzlichen "lebenslangen" Erkennen möglicher Angriffe auf das Speicherbauteil oder Speichermodul vorgesehene Fehlerkorrekturschaltung (<--> "local in-time validation" mittels des Fehlerkorrekturcodes, insbesondere mittels des Hamming-Codes, gemäß der vorliegenden Erfindung), implementiert oder integriert in mindestens ein elektronisches Speicherbauteil oder Speichermodul gemäß der vorstehend dargelegten Art und/oder arbeitend gemäß dem Verfahren gemäß der vorstehend dargelegten Art:

Da die meisten potentiellen Attacken auf Speicherbauteile oder Speichermodule nicht beliebig fokussierbar sind, ist insbesondere infolge der geringen Größe des Speicherzellenbereichs und infolge der Metallabdeckung, die gegebenenfalls zu Streuung der Störungen führt, davon auszugehen, dass gegebenenfalls zumindest ein ganzes Byte betroffen ist. Wird nun in zweckmäßiger Weise dafür gesorgt, dass alle Bits eines Bytes eng beieinander platziert sind, so kann es durch eine Erweiterung bzw. Modifikation der Fehlerkorrekturschaltung ermöglicht werden, dass mit geringem Aufwand entsprechende Angriffe erkannt werden:

So benötigt ein als Fehlerkorrekturcode in bevorzugter Weise gewählter Hamming-Code, der eine Korrektur von Ein-Bit-Fehlern in Speicherzellen ermöglichen soll, eine Hamming-Distanz von 3, das heißt jedes gültige Code- oder Datenwort muss sich von jedem anderen Code- oder Datenwort in mindestens drei Bits unterscheiden (werden zwei gleich lange Binärwörter, zum Beispiel Bytes, miteinander verglichen, dann ist gemäß DIN 44 300 die Anzahl der Bits, in denen sich die beiden gleich langen Binärwörter unterscheiden, die sogenannte "Hamming-Distanz"; dies wird zur Fehlererkennung und zur Fehlerkorrektur benutzt, indem Dateneinheiten, die über die Übertragungsstrecke hereingekommen sind, mit gültigen Zeichen verglichen werden; eine eventuelle Korrektur der Zeichen erfolgt nach dem Wahrscheinlichkeitsprinzip).

Eine Hamming-Distanz von 3 bedeutet, dass für acht Datenbits aufweisende Codewörter oder Datenwörter zusätzlich mindestens vier Redundanzbits erforderlich sind (die Datenbits und die Redundanzbits entsprechen zusammen in erfindungswesentlicher Weise den physikalischen Zuständen P, das heißt der physikalischen Repräsentation). In diesem Zusammenhang ist es möglich bzw. zweckmäßig, den Hamming-Code so zu wählen, dass jedes gültige Zwölf-Bit-Codewort oder Zwölf-Bit-Datenwort mindestens zwei gesetzte Bits (= "1": Zustand "high") und mindestens zwei gelöschte Bits (= "0": Zustand "low") enthält.

Somit hat jedes gültige Zwölf-Bit-Codewort oder Zwölf-Bit-Datenwort eine minimale Hamming-Distanz von 2 zu Sonderzuständen, in denen alle Bits eines Bytes gesetzt (= "1") sind (sogenannter "all-1-Zustand" in bezug auf ein Code- oder Datenwort) oder in denen alle Bits eines Bytes gelöscht (= "0") sind (sogenannter "all-0-Zustand" in bezug auf ein Code- oder Datenwort). Entsprechend sind Daten mit Ein-Bit-Fehlern von diesen Ausnahme- oder Sonderzuständen, die erfindungsgemäß durch den mindestens einen weiteren physikalischen Zustand dargestellt werden und die anhand ihres Bitmusters auf jeden Fall erkannt werden, eindeutig zu unterscheiden.

Bei Verwendung eines solcherart ausgebildeten Fehlerkorrekturcodes können mithin Zustände, in denen alle Bits gesetzt (= "1") sind (sogenannter "all-1-Zustand") bzw. in denen alle Bits gelöscht (= "0") sind (sogenannter "all-0-Zustand"), als ungültige Zustände interpretiert werden. Ein Auftreten derartiger ungültiger Zustände beim Lesen der Daten deutet auf einen das ganze Byte beeinflusst habenden Angriff hin, wie etwa auf ein Beleuchten der Speicherzelle bzw. des Speicherzellenbereichs oder der Leseverstärker ("sense amplifiers") oder auch auf eine komplett gelöschte (und nicht wieder programmierte) Speicherzelle.

Gemäß einer besonders vorteilhaften Weiterbildung der vorliegenden Erfindung ist das Erkennen der Ausnahme- oder Sonderzustände mittels mindestens einer Zwölffach-"and"-Verknüpfung (Zwölffach-"and"-Gate, aufweisend vorzugsweise zwölf Eingänge) bzw. mittels mindestens einer Zwölffach-"nor"-Verknüpfung (Zwölffach-"nor"-Gate, aufweisend vorzugsweise zwölf Eingänge) möglich. In diesem Zusammenhang ist beim Realisieren des Fehlerkorrekturcodes zu berücksichtigen, dass die Testbarkeit des Speicherbausteins, Speicherbauteils oder Speichermoduls gemäß der vorliegenden Erfindung nicht negativ beeinflusst werden darf:

Da beim Testen auch Zustände benötigt werden, in denen alle Bits gesetzt (= "1") sind (sogenannter "all-1-Zustand") bzw. in denen alle Bits gelöscht (= "0") sind (sogenannter "all-0-Zustand"), ist im Testbetrieb eine Umschaltung notwendig, die diese Zustände erlaubt. In zweckmäßiger Weise wird hier ein Fehlerkorrekturcode vorgeschlagen, der im Testmodus wichtige Bitmuster korrekt fortsetzt und im Normalmodus die oben beschriebenen Anforderungen erfüllt:

Testmodus:	Redundanzbit 3 = Parität der Datenbits 7,6,5,4,1
	Redundanzbit 2 = Parität der Datenbits 7,6,3,2,0
	Redundanzbit 1 = Parität der Datenbits 7,5,4,3,0
	Redundanzbit 0 = Parität der Datenbits 6,4,3,2,1

Normalmodus: Redundanzbit 3 = negierte Parität der Datenbits 7,6,5,4,1
Redundanzbit 2 = negierte Parität der Datenbits 7,6,3,2,0
Redundanzbit 1 = negierte Parität der Datenbits 7,5,4,3,0
Redundanzbit 0 = negierte Parität der Datenbits 6,4,3,2,1

Zusammenfassend lässt sich feststellen, dass die vorstehend offenbarte Erweiterung bzw. Modifikation der Fehlerkorrekturschaltung zum zusätzlichen Erkennen möglicher Angriffe auf das Speicherbauteil oder Speichermodul mehrere Vorteile in sich vereint, so unter anderem

- hohe lokale Empfindlichkeit (ein Byte);
- Korrigieren von Ein-Bit-Angriffen (bei intakter Speicherzelle);
- Unabhängigkeit vom Zeitverhalten des Lese- und Störvorgangs;
- keine Erhöhung der Zugriffszeiten;
- Sensitivität auf alle Angriffe, die alle Bits eines Bytes in gleicher Weise beeinflussen;
- kein Erfordernis, die Speichermatrix zu modifizieren;
- sehr geringer Aufwand für das Implementieren des Erkennens der Ausnahme- und Sonderzustände; und
- einfaches Umschalten zwischen Normalmodus und Testmodus.

Was die bevorzugte hardwaretechnische Ausgestaltung der Fehlerkorrekturschaltung anbelangt, so können die beim regulären Programmieren (Schreiben) berechneten bzw. ermittelten Redundanzbits im Normalmodus invertiert und im Testmodus nicht invertiert physikalisch abgelegt werden. Dementsprechend ist gemäß einer vorteilhaften Weiterbildung der vorliegenden Fehlerkorrekturschaltung mindestens eine zum Berechnen bzw. Ermitteln von Redundanzbits bestimmte Berechnungseinheit vorgesehen, der mindestens eine

- mit invertierten Redundanzbits im Normalmodus und/oder
- mit nicht invertierten Redundanzbits im Testmodus

beaufschlagbare Multiplexeinheit nachgeschaltet ist.

Dies bedeutet, dass beim Programmier- oder Schreibvorgang zunächst in zweckmäßiger Weise zu den der Benutzerrepräsentation entsprechenden unkorrigierten Benutzerdaten (= faktisch die Datenbits) die zusätzlichen benötigten Bits mittels der zum Berechnen bzw. Ermitteln von Redundanzbits vorgesehenen Berechnungseinheit berechnet und/oder ermittelt werden.

Diese zusätzlichen benötigten Bits werden in bevorzugter Weise

- im Normalmodus
  - mittels einer dem für den Normalmodus vorgesehenen Eingang einer Multiplexeinheit vorgeschalteten Invertiereinheit invertiert, das heißt negiert und
  - über den Eingang in die Multiplexeinheit geführt bzw.
- im Testmodus
  - nicht invertiert, das heißt nicht negiert und
  - über den für den Testmodus vorgesehenen Eingang der Multiplexeinheit in diese Multiplexeinheit geführt

und von der Multiplexeinheit als Redundanzbits weitergegeben.

Nach Zusammenführen dieser Redundanzbits mit den Benutzerdaten D können diese zusammengeführten Daten als physikalische Daten gespeichert, das heißt physikalisch abgelegt werden.

Um nun im Rahmen des Lesevorgangs den Ausnahme- oder Sonderzustand im Fehlerkorrekturcode zu erkennen, können hardwaretechnisch in erfindungswesentlicher Weise

- mindestens ein mit den Datenbits und mit den Redundanzbits beaufschlagbares Zwölffach-"and"-Gate
  [<--> Interpretieren von Zuständen, in denen alle Bits gesetzt (= "1") sind (sogenannter "all-1-Zustand"), als ungültige Zustände] und/oder
- mindestens ein mit den Datenbits und mit den Redundanzbits

beaufschlagbares Zwölffach-"nor"- Gate

[<--> Interpretieren von Zuständen, in denen alle Bits gelöscht (= "0") sind (sogenannter "all-0-Zustand"), als ungültige Zustände]

vorgesehen sein.

Gemäß einer vorteilhaften Weiterbildung der vorliegenden Fehlerkorrekturschaltung können

- die im Testmodus nicht negierten Redundanzbits und/oder
- die im Normalmodus negierten Redundanzbits (hierzu kann in zweckmäßiger Weise dem für den Normalmodus vorgesehenen Eingang der Multiplexeinheit mindestens eine Invertiereinheit I vorgeschaltet sein)

von mindestens einer mit den Redundanzbits beaufschlagbaren Multiplexeinheit zu mindestens einer der Multiplexeinheit nachgeschalteten Korrektureinheit durchgeschaltet werden.

In bevorzugter Weise berechnet bzw. ermittelt die Korrektureinheit aus den Datenbits die erwarteten Redundanzbits und vergleicht diese erwarteten, vom (Test- bzw. Normal-)Modus unabhängigen Redundanzbits mit den von der Multiplexeinheit durchgeschalteten, im Testmodus nicht negierten bzw. im Normalmodus negierten Redundanzbits. Aus diesem Vergleich lässt sich, wie bei Hamming-Codes üblich, unmittelbar auf ein eventuell falsches Bit schließen, was eine direkte Korrektur durch die Korrektureinheit ermöglicht.

Die vorliegende Erfindung betrifft des weiteren die Verwendung mindestens eines elektronischen Speicherbauteils oder Speichermoduls gemäß der vorstehend dargelegten Art zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen physikalischen Zuständen.

Die vorliegende Erfindung betrifft schließlich die Verwendung des Verfahrens gemäß der vorstehend dargelegten Art zum Implementieren mindestens eines zusätzlichen

Sicherheitsmerkmals in mindestens einer SmartCard, insbesondere in mindestens einer SmartCard-Controllereinheit.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 11 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch die Figuren 2 bis 4B veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1 in schematischer Blockdarstellung den von der Abbildungsfunktion des Fehlerkorrekturcodes vermittelten konventionellen Zusammenhang gemäß dem Stand der Technik zwischen den physikalisch implementierten Bits und den für den Benutzer verfügbaren, gegebenenfalls fehlerkorrigierten Bits;

Fig. 2 in schematischer Blockdarstellung ein Ausführungsbeispiel für eine Erweiterung des Fehlerkorrekturcodes aus Fig. 1 zum Erfassen eines oder mehrerer Ausnahme- oder Sonderzustände gemäß der vorliegenden Erfindung;

Fig. 3 in schematischer, aus Gründen der Übersichtlichkeit sowie der Erkennbarkeit der einzelnen Ausgestaltungen, Elemente oder Merkmale nicht maßstabsgerechter Querschnittsdarstellung ein Ausführungsbeispiel für ein mikroelektronisches Speicherbauteil oder Speichermodul gemäß der vorliegenden Erfindung;

Fig. 4A in schematischer Blockdarstellung ein Ausführungsbeispiel für den auf den Programmier- oder Schreibvorgang bezogenen Teil einer zum Detektieren potentieller Angriffe modifizierten Fehlerkorrekturschaltung gemäß der vorliegenden Erfindung; und

Fig. 4B in schematischer Blockdarstellung ein Ausführungsbeispiel für den auf den Lesevorgang bezogenen Teil einer zum Detektieren potentieller Angriffe modifizierten Fehlerkorrekturschaltung gemäß der vorliegenden Erfindung.

Gleiche oder ähnliche Ausgestaltungen, Elemente oder Merkmale sind in den Figuren 1 bis 4B mit identischen Bezugszeichen versehen.

In Figur 2 ist ein Ausführungsbeispiel für ein Verfahren zum Betreiben eines elektronischen Speicherbausteins 100 (elektronischen Speicherbauteils, elektronischen Speichermoduls) gemäß Figur 3 dargestellt. Bei diesem Verfahren werden reguläre Daten repräsentierende physikalische Zustände P mittels einer einen Fehlerkorrekturcode, nämlich einen Hamming-Code, beschreibenden Abbildungsfunktion A abgebildet.

Gemäß Figur 2 ist der Fehlerkorrekturcode nun dahingegend erweitert, dass auch Ausnahme- oder Sonderzustände S, L im physikalischen Bereich erkannt werden und entsprechend darauf reagiert wird. So kann der Benutzer zum Beispiel den physikalischen Speicher(zellen)bereich 10 mit dem Ausnahme- oder Sonderzustand "gelöscht" programmieren bzw. beschreiben (--> Bezugszeichen S in den Figuren 2 und 4A). Ein späteres Lesen (--> Bezugszeichen L in den Figuren 2 und 4B) desselben Speicherbereichs 10 führt dann zu einer geeigneten Ausnahme bzw. zu einem geeigneten Sonderfall (sogenannte "exception"), falls dieser Ausnahme- oder Sonderzustand nicht zwischenzeitlich wieder mit regulären Daten überschrieben wurde. Dies zwingt den Benutzer zu einer logisch korrekten Reihenfolge der regulären Programmier- bzw. Schreibvorgänge (--> Bezugszeichen S in den Figuren 2 und 4A) und der Lesevorgänge (--> Bezugszeichen L in den Figuren 2 und 4B).

Die Implementation gemäß Figur 2 kann auch dazu genutzt werden, ein nicht-autorisiertes externes Löschen beispielsweise von EPROM-Speicherbausteinen oder

EEPROM-Speicherbausteinen, etwa mit U[ltra]V[iolett]-Licht, als Ausnahme- oder Sonderzustand zu erkennen und dementsprechend zu reagieren.

Alternativ oder in Ergänzung hierzu kann die Implementation gemäß Figur 2 auch dazu genutzt werden, um bewusst Ausnahme- oder Sonderzustände zu erzeugen, bei denen erst deren spätere Löschung das erfolgreiche Ende einer finanziellen Transaktion auf einer Geldkarte signalisiert.

Zusammenfassend lässt sich in bezug auf das Verfahren gemäß Figur 2 also feststellen, dass der Fehlerkorrekturcode exemplarisch erweitert ist, um einen oder mehrere Ausnahme- oder Sonderzustände mitzuerfassen. Die "normalen" Daten des Benutzers programmiert bzw. schreibt und liest dieser in den Registern der gegebenenfalls fehlerkorrigierten Bits K. Der Benutzer hat aber auch die Möglichkeit, einen Ausnahme- oder Sonderzustand selbst zu programmieren bzw. schreiben. In jedem Falle wird der Benutzer durch ein geeignetes Signal davon unterrichtet, wenn er beim Lesevorgang auf der Seite der physikalischen Bits P einen Ausnahme- oder Sonderzustand vorfindet.

Beim anhand Figur 3 veranschaulichten Ausführungsbeispiel eines mikroelektronischen Speicherbausteins 100 auf Halbleiterbasis handelt es sich um einen Flash-Speicherbaustein mit in ein p-dotiertes Aufnahmesubstrat 20 in Form einer HPW-Wanne eingebetteter, das heißt eingelassener Speicherzelle(nmatrix) 10 gemäß der vorliegenden Erfindung.

Dieser Speicherzelle(nmatrix) 10 sind zwei außenliegende Quellen (= Sources) 12a, 12b, eine zentrale Bitline 14, eine zwischen Bitline 14 und erster Quelle 12a bzw. zweiter Quelle 12b angeordnete Wordline 16 sowie ein zwischen Bitline 14 und Wordline liegender Control Gate 18 zugeordnet.

Beim gezeigten Speicherbaustein 100 wird eine hohe Spannung zum Programmieren oder zum Löschen benötigt. Um in diesem Zusammenhang die maximal zu handhabende Spannung so gering wie möglich zu halten, wird die Programmierspannung in einen positiven Anteil und in einen negativen Anteil aufgeteilt. Dies führt dazu, dass das p-dotierte Aufnahmesubstrat 20, in dem die Speicherzellen 10 gebildet werden, auch an ein negatives Potential angeschlossen werden kann.

In den Figuren 4A und 4B ist ein Ausführungsbeispiel für eine gemäß der vorliegenden Erfindung ausgebildete Fehlerkorrekturschaltung 200 dargestellt, die im mikroelektronischen Speicherbaustein 100 gemäß Figur 3 implementiert sowie integriert ist und die zum Detektieren potentieller, auf den Speicherbaustein 100 gerichteter Lichtattacken mittels des Fehlerkorrekturcodes, im speziellen mittels des Hamming-Codes, gemäß der vorliegenden Erfindung bestimmt ist (<--> "local in-time validation for data integrity purposes, especially for security purposes"). In diesem Zusammenhang wird der Fehlerkorrekturcode, nämlich der Hamming-Code, durch die Abbildungsfunktion A (vgl. Figuren 2 und 4B) beschrieben.

Da ein potentieller Beleuchtungsangriff auf das Speicherbauteil oder Speichermodul 100 nicht beliebig fokussierbar ist, ist insbesondere infolge der geringen Größe des Speicherzellenbereichs (= Speicherzellenmatrix 10) davon auszugehen, dass zumindest ein ganzes Byte von einer derartigen Lichtattacke betroffen ist. Da nun dafür gesorgt ist, dass alle Bits eines Bytes eng beieinander platziert sind, kann mittels der Fehlerkorrekturschaltung 200 mit relativ geringem Aufwand ein entsprechender Beleuchtungsangriff erkannt werden:

So benötigt der als Fehlerkorrekturcode gewählte Hamming-Code, der eine Korrektur von Ein-Bit-Fehlern im Speicherzellenbereich 10 ermöglicht, eine Hamming-Distanz von 3, das heißt jedes gültige Code- oder Datenwort unterscheidet sich von jedem anderen Code- oder Datenwort in mindestens drei Bits. Eine Hamming-Distanz von 3 bedeutet, dass für Acht-Bit-Codewörter oder Acht-Bit-Datenwörter D (D0, D1, D2, D3, D4, D5, D6, D7) zusätzlich vier Redundanzbits R (R0, R1, R2, R3) erforderlich sind.

In diesem Zusammenhang ist der Hamming-Code beim Ausführungsbeispiel gemäß Figur 4B so gewählt, dass jedes sich aus dem Acht-Bit-Codewort oder Acht-Bit-Datenwort D (D0, D1, D2, D3, D4, D5, D6, D7) einschließlich der vier Redundanzbits R (R0, R1, R2, R3) ergebende gültige Zwölf-Bit-Codewort oder Zwölf-Bit-Datenwort mindestens zwei gesetzte Bits (= "1": Zustand "high") und mindestens zwei gelöschte Bits (= "0": Zustand "low") enthält.

Somit hat jedes gültige Zwölf-Bit-Codewort oder Zwölf-Bit-Datenwort eine minimale Hamming-Distanz von 2 zu Sonderzuständen, in denen alle Bits eines Bytes gesetzt (= "1") sind (sogenannter "all-1-Zustand" Z1; vgl. Figur 4B) oder in denen alle Bits eines Bytes gelöscht (= "0") sind (sogenannter "all-0-Zustand" Z0; vgl. Figur 4B). Entsprechend sind Daten mit Ein-Bit-Fehlern von diesen Ausnahme- oder Sonderzuständen S bzw. L (vgl. Figuren 2 und 4A bzw. 4B), die durch weitere physikalische Zustände dargestellt werden und die anhand ihres Bitmusters auf jeden Fall erkannt werden, eindeutig zu unterscheiden.

Bei Verwendung des gemäß Figur 4B ausgebildeten Fehlerkorrekturcodes können mithin Zustände, in denen alle Bits gesetzt (= "1") sind (sogenannter "all-1-Zustand") bzw. in denen alle Bits gelöscht (= "0") sind (sogenannter "all-0-Zustand"), als ungültige Zustände interpretiert werden. Ein Auftreten derartiger ungültiger Zustände beim Lesen der Daten deutet auf einen das ganze Byte beeinflusst habenden Angriff hin, wie etwa auf ein Beleuchten der Speicherzelle bzw. des Speicherzellenbereichs 10 oder der Leseverstärker oder auch auf eine komplett gelöschte (und nicht wieder programmierte) Speicherzelle.

Das Erkennen der Ausnahme- oder Sonderzustände S bzw. L (vgl. Figuren 2 und 4A bzw. 4B) ist beim Ausführungsbeispiel für die Fehlerkorrekturschaltung 200 gemäß den Figuren 4A und 4B mittels einer Zwölffach-"and"-Verknüpfung sowie mittels einer Zwölffach-"nor"-Verknüpfung der physikalisch abgelegten Daten P (= Redundanzbits R + Datenbits D) verwirklicht.

Im Detail ist hierbei die Zwölffach-"and"-Verknüpfung in Form eines Zwölffach-"and"-Gates G1 implementiert, das zwölf Eingänge aufweist, nämlich vier Eingänge für die vier Redundanzbits R (R0, R1, R2, R3) und acht Eingänge für die acht Datenbits D (D0, D1, D2, D3, D4, D5, D6, D7). In ähnlicher Weise ist die Zwölffach-"nor"-Verknüpfung in Form eines Zwölffach-"nor"-Gates G0 implementiert, das ebenfalls zwölf Eingänge aufweist, nämlich vier Eingänge für die vier Redundanzbits R (R0, R1, R2, R3) und acht Eingänge für die acht Datenbits D (D0, D1, D2, D3, D4, D5, D6, D7).

Aus der Darstellung gemäß den Figuren 4A und 4B geht in diesem Zusammenhang hervor, dass gemäß der vorliegenden Erfindung die vier Redundanzbits R (R0, R1, R2, R3) und die acht Datenbits D (D0, D1, D2, D3, D4, D5, D6, D7) zusammen den physikalisch gespeicherten bzw. physikalisch implementierten Bits (= physikalische Repräsentation; vgl. Figur 2), das heißt den reguläre Daten repräsentierenden physikalischen Zustände P entsprechen.

Der Fachmann auf dem Gebiet des Designens von Speichermodulen wird in bezug auf das Ausführungsbeispiel gemäß den Figuren 2, 3, 4A und 4B besonders zu schätzen wissen, dass beim Realisieren des Fehlerkorrekturcodes (vgl. Figur 2) die Testbarkeit des Speicherbausteins 100 (vgl. Figur 3) durch die erweiterte Fehlerkorrekturschaltung 200 (vgl. Figuren 4A und 4B) nicht negativ beeinflusst, was wie folgt bewerkstelligt wird:

Da beim Testen (<--> Testmodus T in einer Testeinheit oder Multiplexeinheit M; vgl. Figuren 4A und 4B) auch Zustände benötigt werden, in denen alle Bits gesetzt (= "1") sind (sogenannter "all-1-Zustand" Z1; vgl. Figur 4B) bzw. in denen alle Bits gelöscht (= "0") sind (sogenannter "all-0-Zustand" Z0; vgl. Figur 4B), ist im Testbetrieb eine Umschaltung notwendig, die diese Zustände Z1 und Z0 erlaubt. Aus diesem Grunde wird ein Fehlerkorrekturcode eingesetzt, der im Testmodus T wichtige Bitmuster korrekt fortsetzt und im Normalmodus N die oben beschriebenen Anforderungen erfüllt:

Testmodus T:

Redundanzbit R3 = Parität der fünf Datenbits D7, D6, D5, D4, D1

Redundanzbit R2 = Parität der fünf Datenbits D7, D6, D3, D2, D0

Redundanzbit R1 = Parität der fünf Datenbits D7, D5, D4, D3, D0

Redundanzbit R0 = Parität der fünf Datenbits D6, D4, D3, D2, D1

Normalmodus N:

Redundanzbit R3 = negierte Parität der fünf Datenbits D7, D6, D5, D4, D1

Redundanzbit R2 = negierte Parität der fünf Datenbits D7, D6, D3, D2, D0

Redundanzbit R1 = negierte Parität der fünf Datenbits D7, D5, D4, D3, D0

Redundanzbit R0 = negierte Parität der fünf Datenbits D6, D4, D3, D2, D1

Mittels des mikroelektronischen Speicherbausteins 100 (vgl. Figur 3), insbesondere mittels seiner Speicherzellen(matrix) 10, sowie mittels der im mikroelektronischen Speicherbaustein 100 implementierten oder integrierten Fehlerkorrekturschaltung 200 (vgl. Figuren 4A und 4B), lässt sich das Verfahren gemäß Figur 2 wie folgt verwirklichen:

Zunächst werden gemäß der Darstellung in Figur 4A beim Programmier- oder Schreibvorgang S zu den der Benutzerrepräsentation K entsprechenden, an dieser Stelle naturgemäß unkorrigierten Benutzerdaten (= faktisch die Datenbits D: D0, D1, D2, D3, D4, D5, D6, D7) die zusätzlichen benötigten Bits mittels der zum Berechnen bzw. Ermitteln von Redundanzbits vorgesehenen Berechnungseinheit C berechnet und/oder ermittelt.

Diese zusätzlichen benötigten, über einen ersten Datenbus B1 der Breite 4 geführten Bits werden

- im Normalmodus N

- o mittels einer dem für den Normalmodus N vorgesehenen Eingang EN einer Multiplexeinheit M vorgeschalteten Invertiereinheit I invertiert, das heißt negiert und
- o über den Eingang EN in die Multiplexeinheit M geführt bzw.

- im Testmodus T
  - o nicht invertiert, das heißt nicht negiert und
  - o über den für den Testmodus T vorgesehenen Eingang ET der Multiplexeinheit M in diese Multiplexeinheit M geführt

und von der Multiplexeinheit M als Redundanzbits R: R0, R1, R2, R3 weitergegeben.

Nach Zusammenführen dieser Redundanzbits R mit den über einen zweiten Datenbus B2 der Breite 8 geführten Benutzerdaten D werden diese zusammengeführten Daten als physikalische Daten P gespeichert.

Beim Lesevorgang L gemäß der Darstellung in Figur 4B schaltet die mit den vier Redundanzbits R: R0, R1, R2, R3 über einen ersten Datenbus B1' der Breite 4 beaufschlagte Multiplexeinheit M (vgl. Figur 4B)

- im Testmodus T die nicht negierten Redundanzbits bzw.
- im Normalmodus N die negierten Redundanzbits

zur der Multiplexeinheit M nachgeschalteten Korrektureinheit U (vgl. Figur 4B) durch; hierzu ist dem für den Normalmodus N vorgesehenen Eingang EN der Multiplexeinheit M eine Invertiereinheit I (vgl. Figur 4B) vorgeschaltet. Im Ergebnis werden also die physikalisch gespeicherten Redundanzbits

- im Testmodus T direkt bzw.
- im Normalmodus N "zurück"invertiert

von der Multiplexeinheit M zur Korrektureinheit U durchgeschaltet.

Dies bedeutet mit anderen Worten, dass im Rahmen des Lesevorgangs L die Invertierung über die Invertiereinheit I und die Multiplexeinheit M rückgängig gemacht wird; die vom Testmodus T bzw. vom Normalmodus N folglich gar nichts "wissende"

Korrektureinheit U berechnet und/oder ermittelt aus den über einen zweiten Datenbus B2' der Breite 8 kommenden und an der Korrektureinheit U anliegenden Daten D (= physikalisch gespeicherte Datenbits D0, D1, D2, D3, D4, D5, D6, D7) die erwarteten Redundanzbits (wie beim Schreiben; vgl. Figur 4A) und vergleicht diese erwarteten, vom (Test- bzw. Normal-)Modus unabhängigen Redundanzbits mit den von der Multiplexeinheit M durchgeschalteten gelesenen Redundanzbits R, die im Testmodus T nicht negiert und im Normalmodus N negiert sind. Aus diesem Vergleich lässt sich, wie bei Hamming-Codes üblich, unmittelbar auf ein eventuell fehlerhaftes Bit schließen, was eine direkte Korrektur durch die Korrektureinheit U ermöglicht.

Im Ergebnis verlassen also für den Benutzer verfügbare (fehler)korrigierte Daten K, das heißt die logisch ausgelesene Bits (= Benutzerrepräsentation; vgl. Figuren 2 und 4A bzw. 4B) die der Multiplexeinheit M nachgeschaltete Korrektureinheit U, so dass bei der vorliegenden Erfindung mittels einer begrenzten sowie einfachen Erweiterung einer herkömmlichen Fehlerkorrekturschaltung um die Invertiereinheit I sowie um die Multiplexeinheit M der erwünschte Erfolg erzielt ist.

BEZUGSZEICHENLISTE

100	elektronisches Speicherbauteil oder Speichermodul, insbesondere mikroelektronisches Speicherbauteil oder Speichermodul		
10	Speicherzellenbereich oder Speicherzellenmatrix		
12a	erste Quelle oder erste Source		
12b	zweite Quelle oder zweite Source		
14	Bitline		
16	Wordline		
18	Control Gate		
20	Aufnahmesubstrat		
200	Fehlerkorrekturschaltung		
A	Abbildungsfunktion eines Fehlerkorrekturcodes		
B1	erster Datenbus, insbesondere mit Busbreite 4, beim Programmieren bzw. Schreiben S		
B2	zweiter Datenbus, insbesondere mit Busbreite 8, beim Programmieren bzw. Schreiben S		
B1'	erster Datenbus, insbesondere mit Busbreite 4, beim Lesen L		
B2'	zweiter Datenbus, insbesondere mit Busbreite 8, beim Lesen L		
C	Berechnungseinheit, insbesondere zum Berechnen bzw. Ermitteln von Redundanzbits		
D	acht Datenbits, nämlich	D0	nulltes Datenbit
		D1	erstes Datenbit
		D2	zweites Datenbit
		D3	drittes Datenbit
		D4	viertes Datenbit
		D5	fünftes Datenbit
		D6	sechstes Datenbit
		D7	siebtes Datenbit
EN	für den Normalmodus N vorgesehener Eingang der Multiplexeinheit M		

ET	für den Testmodus T vorgesehener Eingang der Multiplexeinheit M	
G0	Zwölffach-"nor"-Gate	
G1	Zwölffach-"and"-Gate	
I	Invertiereinheit	
K	Benutzerrepräsentation, insbesondere korrigierte Daten, nämlich korrigierte Bits oder logisch ausgelesene Bits	
L	Lesen: Signal an Benutzer (zweiter Ausnahme- oder Sonderzustand)	
M	Multiplexeinheit	
N	Normalmodus	
P	physikalische Repräsentation: physikalische Bits oder physikalisch gespeicherte Bits	
R	vier Redundanzbits, nämlich	R0 nulltes Redundanzbit
		R1 erstes Redundanzbit
		R2 zweites Redundanzbit
		R3 drittes Redundanzbit
S	Programmieren bzw. Schreiben durch Benutzer (erster Ausnahme- oder Sonderzustand)	
T	Testmodus	
U	Korrektureinheit	
Z0	all-0-Zustand, das heißt alle Bits eines Bytes gelöscht (= "0")	
Z1	all-1-Zustand, das heißt alle Bits eines Bytes gesetzt (= "1")	

PATENTANSPRÜCHE

1. Elektronisches Speicherbauteil oder Speichermodul (100), aufweisend mindestens einen Speicherzellenbereich (10), in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming-Code, beschreibenden Abbildungsfunktion (A) abgebildet sind,
gekennzeichnet durch
mindestens einen weiteren, mindestens einen Ausnahme- oder Sonderzustand (L, S) im Fehlerkorrekturcode darstellenden physikalischen Zustand.

2. Speicherbauteil oder Speichermodul gemäß Anspruch 1,
dadurch gekennzeichnet,
dass der Fehlerkorrekturcode und/oder die möglichen Reaktionen auf die verschiedenen physikalischen Zustände hardwaremäßig und/oder softwaremäßig implementiert sind.

3. Speicherbauteil oder Speichermodul gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass der Ausnahme- oder Sonderzustand (L, S) im Fehlerkorrekturcode

- durch das Fließen von Leckströmen bei ausgeschalteten Speicherzellen-transistoren eines jeden Bits;
- als noch nicht beschriebener Speicherblock oder Speicherzellenbereich (10);
- durch Manipulieren des Speicherzellenbereichs (10), etwa durch Bestrahlen des Speicherzellenbereichs (10) mit elektromagnetischen Teilchen oder Wellen; und/oder
- durch das Löschen eines Speicherblocks oder Speicherzellenbereichs (10)

gegeben ist.

4. Speicherbauteil oder Speichermodul gemäß mindestens einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,

- dass der Fehlerkorrekturcode als mindestens ein Hamming-Code ausgebildet ist, der für ein Korrigieren von Ein-Bit-Fehlern im Speicherzellenbereich (10) ausgelegt ist und eine Hamming-Distanz von 3 aufweist, so dass sich jedes gültige Code- oder Datenwort von jedem anderen Code- oder Datenwort in mindestens drei Bits unterscheidet, und
- dass für jedes Acht-Bit-Code- oder Datenwort (D: D0, D1, D2, D3, D4, D5, D6, D7) zusätzlich mindestens vier Redundanzbits (R: R0, R1, R2, R3) vorgesehen sind, so dass sich Zwölf-Bit-Code- oder Datenwörter ergeben.

5. Speicherbauteil oder Speichermodul gemäß Anspruch 4, dadurch gekennzeichnet,

dass der Hamming-Code so ausgelegt ist, dass jedes gültige Zwölf-Bit-Code- oder Datenwort

- mindestens zwei gesetzte Bits (= "1") und/oder
- mindestens zwei gelöschte Bits (= "0")
- aufweist, so dass jedes gültige Zwölf-Bit-Code- oder Datenwort eine minimale Hamming-Distanz von 2 zu Sonderzuständen hat,
- in denen alle Bits eines Bytes gesetzt (= "1") sind (Z1) bzw.
- in denen alle Bits eines Bytes gelöscht (= "0") sind (Z0).

6. Speicherbauteil oder Speichermodul gemäß Anspruch 4 oder 5, dadurch gekennzeichnet,

dass die vier Redundanzbits (R: R0, R1, R2, R3)

- im auch Zustände, in denen alle Bits eines Bytes gesetzt (= "1") sind (Z1) oder in denen alle Bits eines Bytes gelöscht (= "0") sind (Z0), umfassenden Testmodus (T) wie folgt gewählt sind:

-- drittes Redundanzbit (R3) entspricht Parität des siebten Datenbits (D7),

des sechsten Datenbits (D6),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des ersten Datenbits (D1);

-- zweites Redundanzbit (R2) entspricht Parität des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des nullten Datenbits (D0);

-- erstes Redundanzbit (R1) entspricht Parität des siebten Datenbits (D7),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des nullten Datenbits (D0);

-- nulltes Redundanzbit (R0) entspricht Parität des sechsten Datenbits (D6),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des ersten Datenbits (D1); und/oder

- im Normalmodus (N) wie folgt gewählt sind:

-- drittes Redundanzbit (R3) entspricht negierter Parität
des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des ersten Datenbits (D1);

-- zweites Redundanzbit (R2) entspricht negierter Parität
des siebten Datenbits (D7),
des sechsten Datenbits (D6),

des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des nullten Datenbits (D0);

-- erstes Redundanzbit (R1) entspricht negierter Parität
des siebten Datenbits (D7),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des nullten Datenbits (D0);

-- nulltes Redundanzbit (R0) entspricht negierter Parität
des sechsten Datenbits (D6),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des ersten Datenbits (D1).

7. Speicherbauteil oder Speichermodul gemäß mindestens einem der Ansprüche 4 bis 6, dadurch gekennzeichnet,
dass die Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und die Redundanzbits (R: R0, R1, R2, R3) zusammen den physikalischen Zuständen (P) entsprechen.

8. Speicherbauteil oder Speichermodul gemäß mindestens einem der Ansprüche 1 bis 7, dadurch gekennzeichnet,
dass der Speicherzellenmatrix (10)

- mindestens eine Quelle oder Source (12a, 12b),
- mindestens eine Bitline (14),
- mindestens eine Wordline (16) und
- mindestens ein Control Gate (18)

zugeordnet ist.

9. Speicherbauteil oder Speichermodul gemäß mindestens einem der Ansprüche 1 bis 8, dadurch gekennzeichnet,
dass das Speicherbauteil oder Speichermodul (100)

- als E[rasable]P[rogrammable]R[ead]O[nly]M[emory],
- als E[lectrically]E[rasable]P[rogrammable]R[ead]O[nly]M[emory],
- als Flash-Speicher,
- als R[ead]O[nly]M[emory] oder
- als R[andom]A[ccess]M[emory]

ausgebildet ist.

10. Verwendung mindestens eines elektronischen Speicherbauteils oder Speichermoduls (100) gemäß mindestens einem der Ansprüche 1 bis 9 zum Erkennen und/oder zum Markieren von ungültigen oder anderweitig speziellen physikalischen Zuständen.

11. Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils oder Speichermoduls, insbesondere gemäß mindestens einem der Ansprüche 1 bis 9, in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming-Code, beschreibenden Abbildungsfunktion (A) abgebildet werden,
dadurch gekennzeichnet,
dass mittels der Abbildungsfunktion (A) mindestens ein weiterer physikalischer Zustand in Form mindestens eines Ausnahme- oder Sonderzustands (L, S) im Fehlerkorrekturcode erfasst, kodiert und/oder signalisiert werden kann.

12. Verfahren gemäß Anspruch 11,
dadurch gekennzeichnet,
dass der weitere physikalische Zustand anhand seines Bitmusters auch im Falle einer für die regulären Daten geltenden eingeschränkten Fehlererkennung bzw. -korrektur erfasst, kodiert und/oder signalisiert werden kann.

13. Verfahren gemäß Anspruch 11 oder 12,
gekennzeichnet durch
mindestens eine redundante Datenkodierung.

14. Verfahren gemäß mindestens einem der Ansprüche 11 bis 13,
dadurch gekennzeichnet,

- dass als Fehlerkorrekturcode mindestens ein für ein Korrigieren von Ein-Bit-Fehlern im Speicherzellenbereich (10) bestimmter Hamming-Code mit einer Hamming-Distanz von 3 gewählt wird, so dass sich jedes gültige Code- oder Datenwort von jedem anderen Code- oder Datenwort in mindestens drei Bits unterscheidet, und
- dass für jedes Acht-Bit-Code- oder Datenwort (D: D0, D1, D2, D3, D4, D5, D6, D7) zusätzlich mindestens vier Redundanzbits (R: R0, R1, R2, R3) vorgesehen sind, so dass Zwölf-Bit-Code- oder Datenwörter gebildet werden.

15. Verfahren gemäß Anspruch 14,
dadurch gekennzeichnet,
dass der Hamming-Code so gewählt wird, dass jedes gültige Zwölf-Bit-Code- oder Datenwort

- mindestens zwei gesetzte Bits (= "1") und/oder
- mindestens zwei gelöschte Bits (= "0")
- aufweist, so dass jedes gültige Zwölf-Bit-Code- oder Datenwort eine minimale Hamming-Distanz von 2 zu Sonderzuständen hat,
- in denen alle Bits eines Bytes gesetzt (= "1") werden (Z1) oder
- in denen alle Bits eines Bytes gelöscht (= "0") werden (Z0).

16. Verfahren gemäß Anspruch 14 oder 15,
gekennzeichnet

- durch mindestens eine mit den Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und mit den Redundanzbits (R: R0, R1, R2, R3) beaufschlagbare Zwölffach-"and"-Verknüpfung und/oder
- durch mindestens eine mit den Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und mit den Redundanzbits (R: R0, R1, R2, R3) beaufschlagbare Zwölffach-"nor"-Verknüpfung
- zum Erkennen des Ausnahme- oder Sonderzustands (L, S) im Fehlerkorrekturcode.

17. Verfahren gemäß mindestens einem der Ansprüche 14 bis 16,
dadurch gekennzeichnet,
dass die vier Redundanzbits (R: R0, R1, R2, R3)

- im auch Zustände, in denen alle Bits eines Bytes gesetzt (= "1") werden (Z1) oder in denen alle Bits eines Bytes gelöscht (= "0") werden (Z0), umfassenden Testmodus (T) wie folgt gewählt werden:

-- drittes Redundanzbit (R3) entspricht Parität des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des ersten Datenbits (D1);

-- zweites Redundanzbit (R2) entspricht Parität des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des nullten Datenbits (D0);

-- erstes Redundanzbit (R1) entspricht Parität des siebten Datenbits (D7),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des dritten Datenbits (D3),

des nullten Datenbits (D0);

-- nulltes Redundanzbit (R0) entspricht Parität des sechsten Datenbits (D6),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des ersten Datenbits (D1); und/oder

- im Normalmodus (N) wie folgt gewählt werden:

-- drittes Redundanzbit (R3) entspricht negierter Parität
des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des ersten Datenbits (D1);

-- zweites Redundanzbit (R2) entspricht negierter Parität
des siebten Datenbits (D7),
des sechsten Datenbits (D6),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des nullten Datenbits (D0);

-- erstes Redundanzbit (R1) entspricht negierter Parität
des siebten Datenbits (D7),
des fünften Datenbits (D5),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des nullten Datenbits (D0);

-- nulltes Redundanzbit (R0) entspricht negierter Parität
des sechsten Datenbits (D6),
des vierten Datenbits (D4),
des dritten Datenbits (D3),
des zweiten Datenbits (D2),
des ersten Datenbits (D1).

18. Verfahren gemäß mindestens einem der Ansprüche 14 bis 17,
dadurch gekennzeichnet,
dass die Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und die Redundanzbits (R: R0, R1, R2, R3) zusammen den physikalischen Zuständen (P) entsprechen.

19. Fehlerkorrekturschaltung (200), implementiert oder integriert in mindestens ein elektronisches Speicherbauteil oder Speichermodul (100) gemäß mindestens einem der Ansprüche 1 bis 9 und/oder arbeitend gemäß dem Verfahren gemäß mindestens einem der Ansprüche 11 bis 18.

20. Fehlerkorrekturschaltung gemäß Anspruch 19,
gekennzeichnet durch
mindestens eine zum Berechnen bzw. Ermitteln von Redundanzbits (R: R0, R1, R2, R3) vorgesehene Berechnungseinheit (C), der mindestens eine

- mit nicht invertierten Redundanzbits im Testmodus (T) und/oder
- mit invertierten Redundanzbits im Normalmodus (N)

beaufschlagbare Multiplexeinheit (M) nachgeschaltet ist.

21. Fehlerkorrekturschaltung gemäß Anspruch 19 oder 20,
gekennzeichnet

- durch mindestens ein mit den Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und mit den Redundanzbits (R: R0, R1, R2, R3) beaufschlagbares Zwölffach-"and"-Gate (G1) und/oder
- durch mindestens ein mit den Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) und mit den Redundanzbits (R: R0, R1, R2, R3) beaufschlagbares Zwölffach-"nor"-Gate (G0)

zum Erkennen des Ausnahme- oder Sonderzustands (L, S) im Fehlerkorrekturcode.

22. Fehlerkorrekturschaltung gemäß mindestens einem der Ansprüche 19 bis 21, gekennzeichnet durch
mindestens eine mit den Redundanzbits (R: R0, R1, R2, R3) beaufschlagbare Multiplexeinheit (M) zum Durchschalten
- der nicht negierten Redundanzbits im Testmodus (T) und/oder
- der negierten Redundanzbits im Normalmodus (N)

zu mindestens einer der Multiplexeinheit (M) nachgeschalteten Korrektureinheit (U).

23. Fehlerkorrekturschaltung gemäß Anspruch 20 oder 22, gekennzeichnet durch
mindestens eine dem für den Normalmodus (N) vorgesehenen Eingang (EN) der Multiplexeinheit (M) vorgeschaltete Invertiereinheit (I).

24. Fehlerkorrekturschaltung gemäß Anspruch 22 oder 23, dadurch gekennzeichnet,
dass die Korrektureinheit (U) aus den Datenbits (D: D0, D1, D2, D3, D4, D5, D6, D7) die erwarteten Redundanzbits berechnet und/oder ermittelt und diese erwarteten Redundanzbits mit den von der Multiplexeinheit (M) durchgeschalteten, im Testmodus (T) nicht negierten bzw. im Normalmodus (N) negierten Redundanzbits (R: R0, R1, R2, R3) vergleicht.

25. Verwendung des Verfahrens gemäß mindestens einem der Ansprüche 11 bis 18 zum Implementieren mindestens eines zusätzlichen Sicherheitsmerkmals in mindestens einer SmartCard, insbesondere in mindestens einer SmartCard-Controllereinheit.

ZUSAMMENFASSUNG

Elektronisches Speicherbauteil oder Speichermodul und Verfahren zum Betreiben desselben

Um ein elektronisches Speicherbauteil oder Speichermodul (100), aufweisend mindestens einen Speicherzellenbereich (10), in dem reguläre Daten repräsentierende physikalische Zustände (P) mittels mindestens einer mindestens einen Fehlerkorrekturcode, zum Beispiel mindestens einen Hamming-Code, beschreibenden Abbildungsfunktion (A) abgebildet sind, sowie ein Verfahren zum Betreiben mindestens eines elektronischen Speicherbauteils oder Speichermoduls (100) der vorgenannten Art so weiterzubilden, dass zum einen die Wahrscheinlichkeit einer Fehlererkennung deutlich erhöht ist und zum anderen unbeschriebene Speicherblöcke in zuverlässiger Weise von schon einmal beschriebenen Speicherblöcken unterschieden werden können, wird vorgeschlagen, dass mittels der Abbildungsfunktion (A) mindestens ein weiterer physikalischer Zustand in Form mindestens eines Ausnahme- oder Sonderzustands (L, S) im Fehlerkorrekturcode erfasst, kodiert und/oder signalisiert werden kann.

Fig. 2

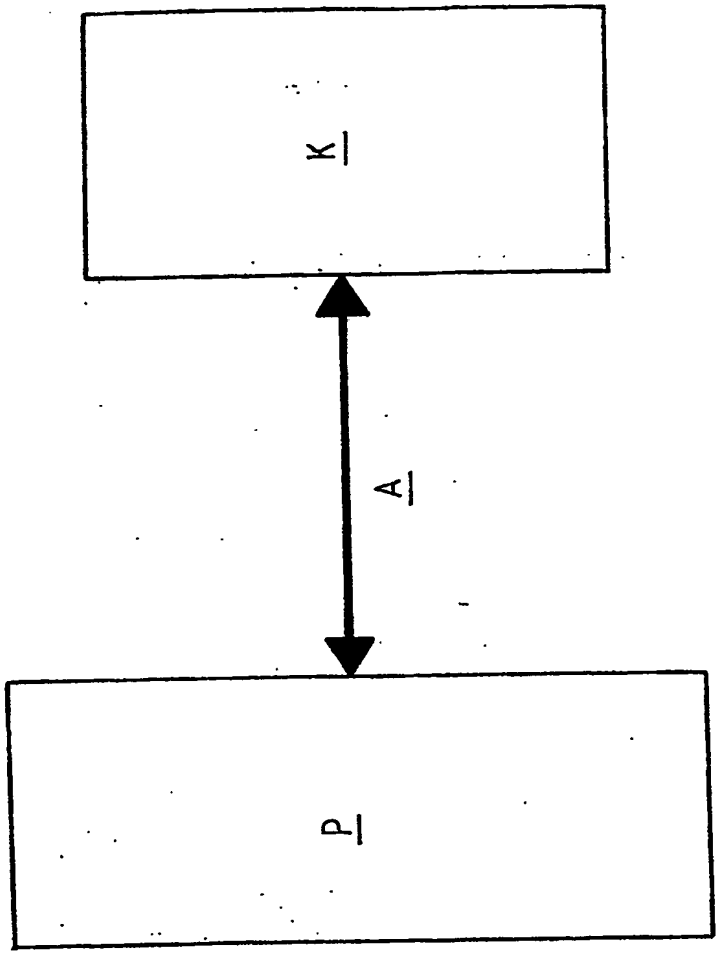

Fig.1

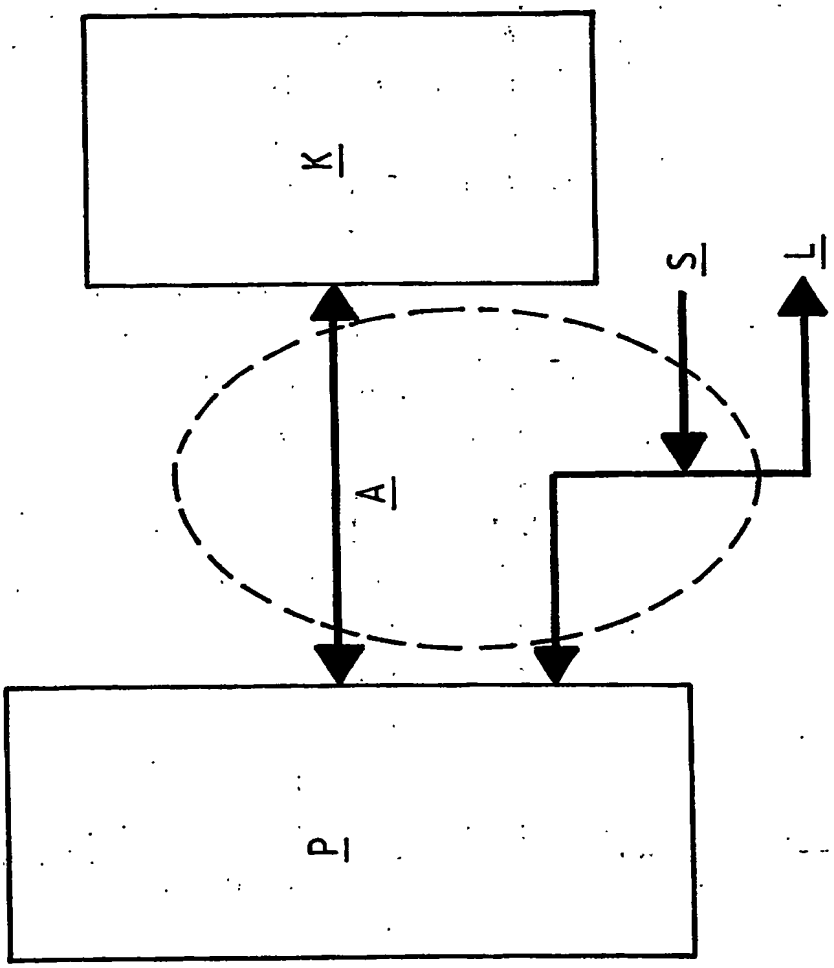

Fig.2

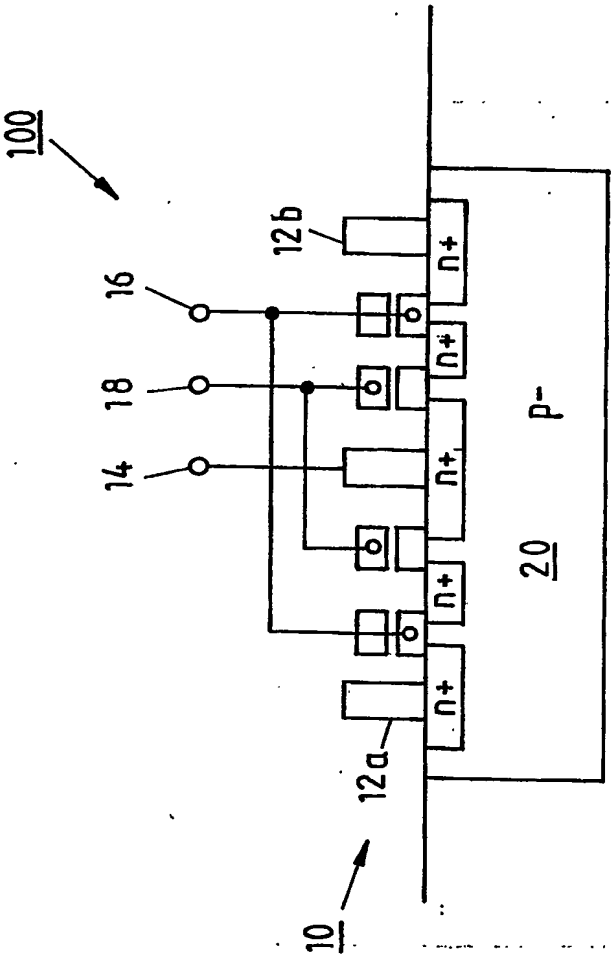

Fig.3

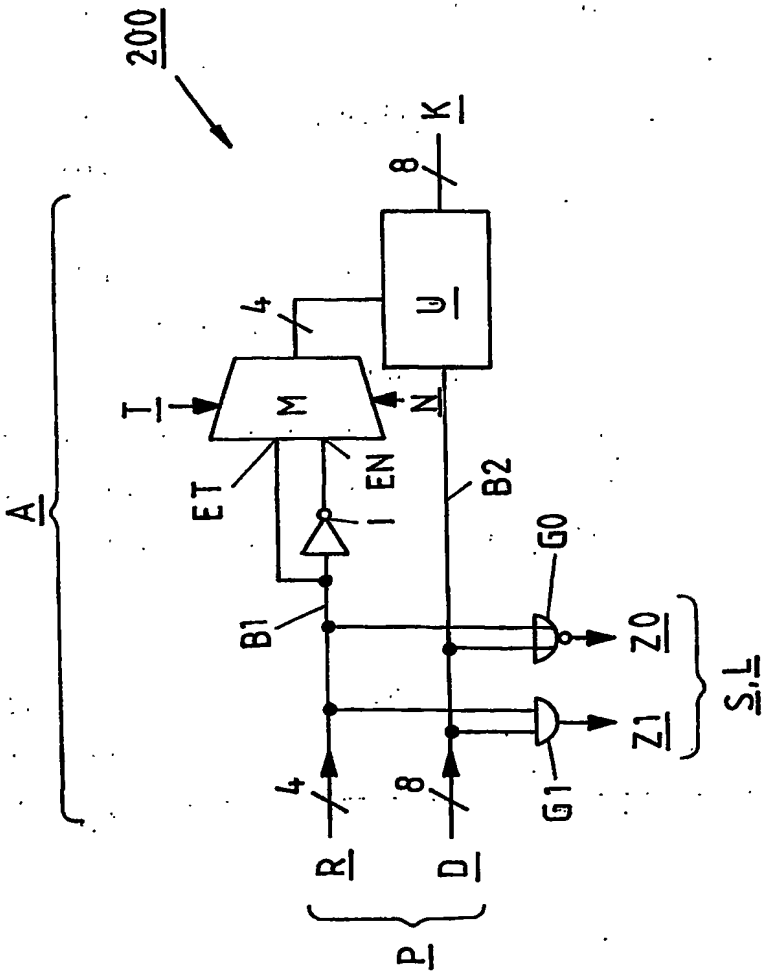

Fig.4